Cyber Preparedness and Response
At the Local Level

Statement of

Chief Sam Greif
Plano (TX) Fire-Rescue Department

presented to the

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION & SECURITY TECHNOLOGIES

OF THE

COMMITTEE ON HOMELAND SECURITY

U.S. House of Representatives

April 7, 2016

International Association of Fire Chiefs
4025 Fair Ridge Drive • Fairfax, VA 22033-2868

Good morning, Chairman Ratcliffe, Ranking Member Richmond, and members of the subcommittee. I am Chief Sam Greif of the Plano Fire-Rescue Department. Today I am pleased to testify on behalf of the International Association of Fire Chiefs. The IAFC represents more than 11,000 leaders of the nation's fire, rescue, and emergency medical services. Thank you for the opportunity to discuss important issues related to cybersecurity and the fire and emergency service. This is a growing threat that adds yet another mission for the America's firefighters and emergency medical personnel.

The Problem of Cybersecurity

Cybercrime and cyber-attacks are becoming a more prevalent threat to the American homeland. A 2010 report by Norton found that two-thirds of the world's population have been the victim of some form of cybercrime. A 2009 study by McAfee demonstrated that cybercrime, including security breaches and data theft, may have cost international business has much as $1 trillion. We have seen how cyber-attacks can harm major universities, medical facilities, financial institutions, retailers, local governments and federal agencies.

The fire and emergency service is just beginning to recognize how these threats can affect our operations. There have been attempts to use robocalls and other denial of service attacks to affect operations at 9-1-1 Public Safety Answering Points (PSAP). Just recently, we have seen a rash of cyber-attacks against hospitals in California, Kentucky, and the Washington, D.C. area. In addition, we always must be vigilant for malware, phishing, spammers, and spyware which are aimed at infiltrating and debilitating our systems.

From the fire and emergency service's perspective, it is important that we protect vital systems that support our operations. The 9-1-1 systems are necessary for the public to call and request assistance during emergency situations. Computer-aided dispatch (CAD) systems are essential for determining which units are available to respond and assigning them to an incident scene. These units must be able to communicate with the dispatch center, command units and each other effectively at the incident scene. In addition, patient reporting information must be protected by the emergency medical service (EMS), because of the nature of the data. As the nation transforms to a more digital world and the "Internet of Things," all of these capabilities will be presented with an increasing number of opportunities to provide service to our citizens and a corresponding number of vulnerabilities to cyber threats.

Protecting the Fire and Emergency Service

As they consider the various threats to their computer systems, fire and EMS departments must take steps to protect themselves. Before I became fire chief in Plano, I served for 30 years in the Fort Worth Fire Department, where I oversaw the city's 9-1-1 center for 10 years. One of our major missions was to protect our CAD and 9-1-1 systems from cyber-attacks. To protect our systems, we segregated them from the outside world. This action minimized the ability of outsiders to compromise our systems through the internet. To update our systems, we would have to go to the server and install software manually. It is important to recognize, though, that most of a fire and EMS department's computer systems, like human resources, email and finance, will be part of the overall jurisdiction's information technology (IT) systems.

Fire and EMS departments also have to take steps to harden their systems. In order to protect their 9-1-1 systems from massed robocalls aimed at taking down the system, the departments have to constantly test their systems' vulnerabilities to make sure that they can withstand heavy call volumes. The fire departments also have to download and use a testbed to evaluate all software before installing it. It is important to realize that – as communications systems move to digital systems that use VoIP – these systems need to be secure from cyber-attacks that might compromise lifesaving operations on the fire scene. In addition, 9-1-1 Public Safety Answering Points (PSAP) should be constructed to be secure from outside attacks and have resilient systems and back-up power.

As with other threats, local fire and EMS chiefs must stay aware of new threats and prepare for them. The best way to stay informed is to develop relationships with intelligence fusion centers, federal officials and local law enforcement. If fire and EMS departments can support the staffing requirements, they should have personnel stationed at the state and local fusion centers. Grants administered by the Federal Emergency Management Agency (FEMA), including the State Homeland Security Grant Program (SHSGP) and Urban Areas Security Initiative (UASI), will support fire and emergency service personnel in fusion centers. Fire and EMS departments also should maintain close relationships with local Joint Terrorism Task Forces. These resources will keep fire and EMS chiefs informed on the latest cyber threats and help them address any vulnerabilities.

It also is important to develop close working relationships with local law enforcement officials. In Fort Worth, I worked with the local police intelligence unit, which was aware of new threats to the community. In Plano, the public safety group, composed of the city communications director, the police chief, the emergency manager and me, meet monthly to discuss threats and how to prepare for them.

Federal information sharing systems, like the Homeland Security Information Network (HSIN), also can provide important information about cyber threats and how to prepare for them. HSIN is a national, secure, web-based portal for information-sharing and collaboration between federal, state, local, tribal, territorial, and private sector partners. HSIN has a community of interest dedicated to the fire and emergency service. The U.S. Department of Homeland Security (DHS) must make sure that cybersecurity-related information is added to this community of interest, so that local fire and EMS chiefs can access it.

Since fire and EMS departments depend on mutual aid to respond to major incidents, they should address cybersecurity concerns as part of their planning and training. Communications must be interoperable during an incident; a breakdown in communications or dispatch systems during an incident could cause confusion at a critical time. To address this risk, the North Central Texas Council of Governments addressed cybersecurity as part of its interoperability plans. For Super Bowl XLV in 2011, the Multi-Quad County Consortium developed a communications plan that addressed cybersecurity concerns and developed plans for responding to a cyber-attack.

Finally, training and exercises are key to preventing and responding to an incident. One of the basic ways to protect computer systems is to train staff not to click on spam ware, malware, or spoofing attacks. In addition, fire and EMS departments must ensure that all of their virus software is up-to-date. These are simple tasks that can protect a system. Fire and EMS departments also can audit their systems to evaluate vulnerabilities. It also is worthwhile to study the effects of cyber-attacks on other public safety organizations to see how their operations were affected and what they did to mitigate the damage. Local fire and EMS departments can work with local law enforcement agencies, emergency managers and the jurisdictions' IT staff to plan and exercise contingency plans in case of cyber-attacks aimed at taking down key systems.

The Federal Government's Role

The federal government can be an important partner. Most importantly, it can help educate fire and EMS departments about the cybersecurity threat. The DHS' Office of Cybersecurity and Communications (C&SC) can work with FEMA to raise awareness in local fire departments about the threats that cyber-attacks can pose. The U.S. Fire Administration (USFA) is an agency within FEMA that supports the local fire and emergency service. By working with USFA and its National Fire Academy, C&SC can develop education and training to help fire and EMS departments learn how to determine which systems might be vulnerable to cyber-attacks and make the necessary changes to protect them. It is important to note that the President's Fiscal Year (FY) 2017 budget proposes to cut USFA by $1.7 million. We recommend that – instead – Congress fund USFA at the FY 2011 level of $45.6 million, so that the agency can develop training for emerging threats like cybersecurity.

Also, DHS can continue to support training and exercises to help fire and EMS departments prepare for the threat of a cyber-attack. A cyber-related component can be added to the state and local exercises. In addition, DHS should continue to support state and local fusion centers, which serve an important purpose in sharing threat information. These programs are funded though the SHSGP and UASI programs. Unfortunately, the President's FY 2017 budget proposes to cut these programs drastically. The budget would cut the SHSGP program to $200 million (a decrease of more than 50%) and the UASI program would be cut to $330 million (a 45% cut). We urge Congress to fund these programs – at least – at the FY 2016 level of $467 million for the SHSGP program and $600 million for the UASI program.

Recently, the DHS National Protection and Programs Directorate (NPPD) announced a proposal to realign itself to have a greater focus on cybersecurity. Overall, the IAFC is supportive of this proposal. However, we have concerns about how this realignment would affect the Office of Emergency Communications (OEC). The OEC's mission is to promote public safety communications interoperability using a local stakeholder-directed approach. The IAFC and other public safety organizations do not support efforts to move OEC under the Infrastructure Security component. Instead, we recommend that OEC remain a separate component within NPPD.

Conclusion

Thank you for the opportunity to testify at today's hearing. Cybersecurity is an issue of growing importance to the nation. A breakdown of a fire and EMS department's CAD or communications system during the response to an incident could result in tragic consequences. It is important that local fire and EMS departments strengthen their systems to protect them. In addition, fire and EMS chiefs should develop strong working relationships with federal, state, and local law enforcement officials to be aware of emerging threats. Finally, local fire and EMS chiefs should make sure that their staff are trained in basic cybersecurity safety, and plan and exercise for the consequences of a successful cyber-attack. Taking these necessary precautions should help local fire and EMS departments to adapt to this emerging threat.